



PTO/SB/08a/b (08-03)

Approved for use through 07/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Application Number	10/825,625-Conf. #7860
				Filing Date	April 15, 2004
				First Named Inventor	Wieland Fischer
				Art Unit	N/A
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	20193/0201102-USO

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
/COI	1	US-6,092,229-B1	07-18-2000	Boyle et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ³
		Country Code ⁴ -Number ⁴ -Kind Code ⁴ (if known)	MM-DD-YYYY			
/COI	2	EP-0 743 774-A2	11-20-1996	Certicom Corp.		
I	3	EP-0 872 795-A1	10-21-1998	Mykotronx, Inc.		
	4	DE-42 34 165-C1	03-03-1994	Detecon GmbH		
	5	DE-197 25 167-A1	12-17-1998	Utimaco Safeware AG		
	6	DE-199 61 838-A1	07-05-2001	SCM Microsystems GmbH		
/COI	7	EP-0 621 569-B1	07-14-1999			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS					
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.			T ²
/COI	8	Wu, Chung-Hsien, et al., "RSA Cryptosystem Design Based on the Chinese Remainder Theorem", IEEE, 2001, pp. 391-395.			
	9	Comba, P.G., "Exponentiation cryptosystems on the IBM PC", IBM Systems Journal, 1990, Vol. 29, No. 4, pp. 526-538.			
	10	Shand, M., et al., "Fast Implementations of RSA Cryptography", 11th Symposium on Computer Arithmetic, June 29-July 2, 1993, pp. 252-259.			
	11	Grossshadi, Johann, "High-Speed RSA Hardware Based on Barret's Modular Reduction Method", 2000, pp. 191-203.			
	12	Quisquater, J., et al., "Fast Decipherment Algorithm For RSA Public-Key Cryptosystem", Electronics Letters, October 1982, Vol. 18, No. 21, pp. 905-907.			
	13	Bao, F., et al., "Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults", Proceedings of the 5th Workshop on Secure Protocols, LNCS 1361, April 7-9, 1997, pp. 115-124.			
	14	Klima, Vlastimil, et al., "Attack on Private Signature Keys of the OpenPGP format, PGP TM programs and other applications compatible with OpenPGP", March 22, 2001, pp. 1-20.			
	15	Rankl, Wolfgang, et al., "Handbuck der Chipkarten", pp. 138-139.			
	16	Boneh, Dan, et al., "On the Importance of Eliminating Errors in Cryptographic Computations", Journal of Cryptology, 2001, Vol. 14, pp. 101-119.			
/COI	17	Shamir, A., "How to check modular exponentiation", Oral publication.			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature	/Chinwendu Okoronkwo/	Date Considered	09/29/2007
--------------------	-----------------------	-----------------	------------

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete If Known	
				Application Number	Not Yet Assigned
				Filing Date	Concurrently Herewith
				First Named Inventor	Wieland Fischer
				Art Unit	N/A
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	20046/0201102-USO

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/CO/	AA	US-5,991,415-B1	11-23-1999	Shamir	
/CO/	AB	US-6,282,290-B1	08-28-2001	Powell et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
		Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)	MM-DD-YYYY			
/CO/	BA	DE-100 24 325-A1	12-06-2001	Seysen		x

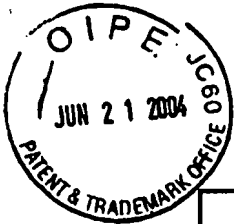
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS					T ²
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.			
/CO/	CA	Bong D et al: "OPTIMIZED SOFTWARE IMPLEMENTATIONS OF THE MODULAR EXPONENTIATION ON GENERAL PURPOSE MICROPROCESSORS"; Computers & Security, International Journal Devoted to the Study of Technical and Financial Aspects of Computer Security, Elsevier Science Publishers, Amsterdam, NL, Vol. 8, No. 7, 1 November 1989, Pages 621-630.			
	CB	Boneh D et al: "ON THE IMPORTANCE OF CHECKING CRYPTOGRAPHIC PROTOCOLS FOR FAULTS"; Advances in Cryptology, Eurocrypt, 11 May 1997, Pages 37-51.			
	CC	Schindler W: "A TIMING ATTACK AGAINST RSA WITH THE CHINESE REMAINDER THEOREM"; Cryptographic Hardware and Embedded Systems, 2nd International Workshop, CHES 2000, Worcester, MA, August 17-18, 2000 Proceedings, Lecture Notes in Computer Science, Berlin: Springer, Germany, Pages 109-124.			
	CD	Grossschadi J: "THE CHINESE REMAINDER THEOREM AND ITS APPLICATION IN A HIGH-SPEED RSA CRYPTO CHIP"; Computer Security Applications, 2000. ACSAC '00, 16th Annual Conference, New Orleans, LA, December 11-15, 2000, Los Alamitos, CA, IEEE Comput. Soc, 11 December 2000, pages 384-393.			
	CE	Schnorr C: "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS"; Lecture Notes in Computer Science, Vol. 434, Berlin, Springer, 1990, pages 239-252.			
	CF	Boneh D et al.: "ON THE IMPORTANCE OF CHECKING CRYPTOGRAPHIC PROTOCOLS FOR FAULTS"; Lecture Notes in Computer Science, Vol. 1233, Berlin, Springer, 1997, pages 37-51.			
/CO/	CG	Menezes A.J.: "HANDBOOK OF APPLIED CRYPTOGRAPHY"; Boca Raton, FL. CRC Press, 1997, pages 612-613.			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature	/Chinwendu Okoronkwo/	Date Considered	09/29/2007
--------------------	-----------------------	-----------------	------------



PTO/SB/08a/b (08-03)

Approved for use through 07/31/2008. OMB 0851-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use as many sheets as necessary)				Complete if Known	
				Application Number	10/825,625
				Filing Date	April 15, 2004
				First Named Inventor	Wieland Fischer
				Art Unit	N/A
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	20193/0201102-USO

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ -Number-Kind Code ⁴ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/COI/	CA	Menezes A.J. et al; "RSA public-key encryption"; HANDBOOK OF APPLIED CRYPTOGRAPHY; CRC Press 1996, Chapter 8.2.	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature	/Chinwendu Okoronkwo/	Date Considered	09/29/2007
-----------------------	-----------------------	--------------------	------------

Substitute for form 1449A/B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Application Number	10/825,625-Conf. #7860
				Filing Date	April 19, 2004
				First Named Inventor	Wieland Fischer
				Art Unit	Not Yet Assigned
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	S0193.00197

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T ⁶
/CO/	BA	-DE 199 44 991 A1 (corresponds to U.S. Patent 6,934,887)	04-12-2001	Baldischweiler		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.18 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
/CO/	CA	Rankl et al., "Handbuch der Chipkarten", Vol. 3, Hanser Verlag, pgs. 506-509 (w/English translation of relevant portion)	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature	/Chinwendu Okoronkwo/	Date Considered	09/29/2007
-----------------------	-----------------------	--------------------	------------

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	10/825,625-Conf. #7860
				Filing Date	April 15, 2004
				First Named Inventor	Wieland Fischer
				Art Unit	2131
				Examiner Name	A. R. Sheikh
Sheet	1	of	1	Attorney Docket Number	S0193.0017

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
/CO/	AA*	US-5,631,960	05-20-1997	Likens et al.	
	AB*	US-6,144,740	11-07-2000	Laih et al.	
	AC*	US-5,991,415	11-23-1999	Shamir et al.	
	AD*	US-6,965,673	11-15-2005	Boneh et al.	
/CO/	AE*	US-6,986,050-A1	01-10-2006	Hypponen et al.	

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. * CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature	/Chinwendu Okoronkwo/	Date Considered	09/29/2007
-----------------------	-----------------------	--------------------	------------